(corresponding to US 5,442,645)

⑲日本国特許庁(JP)　　⑪特許出願公表　⑯

⑫公表特許公報(A)　　平3－503220

㊸公表　平成3年(1991)7月18日

㊶Int.Cl.⁵		識別記号	庁内整理番号
G 06 F	12/14	310 Z	7737－5B
	9/06	450 Z	7927－5B
	11/10	330 K	9072－5B

審査請求　有
予備審査請求　未請求　　部門(区分)　6(3)

(全15頁)

㊹発明の名称　プログラムまたはデータの完全性をチエツクする方法及び該方法を実施するシステム

㉑特　願　平2－508410
㉒㉓出　願　平2(1990)6月1日
㉕翻訳文提出日　平3(1991)2月6日
㉖国際出願　PCT/FR90/00381
㉗国際公開番号　WO90/15384
㉘国際公開日　平2(1990)12月13日

優先権主張　㉜1989年6月6日㉝フランス(FR)㉞89/07429

㉒発明者　ユゴン，ミツシエル　フランス国、78310・モルパ、リユ・デ・セバージユ、6
㉒発明者　オアゼル，アンドレ　フランス国、78990・エランクール、レ・ヌーボー・オリゾン、5
㉑出願人　ブル・セー・ベー・8　フランス国、78190・トラツブ、リユ・ユジエーヌ・エナフ　(番地なし)
㉔代理人　弁理士　川口　義雄　外4名
㉛指定国　CA,JP,KR,US

請求の範囲

1．コンピュータプログラム及び/またはコンピュータデータの命令のごとき情報を含むメッセージをオリジナルメッセージに対して比較することによって前記メッセージの完全性をチェックするために、処理回路が、オリジナルメッセージ(M)に変換アルゴリズム(A)を適用してサイン(S)を計算するタイプの方法であって、処理回路がメッセージの少なくとも一部を抽出し、アルゴリズム(A)の適用によって前記メッセージ部の関数である少なくとも1つのサインを(S1,S2....Sn)を計算する段階と、処理回路(11)と該処理回路(11)だけがアクセスできる少なくとも1つの非揮発性記憶領域(10)とを内蔵する携帯電子装置をオリジナルメッセージに結合させ、アルゴリズム(A)を実行し得る処理回路の制御下にオリジナルメッセージの各サイン(S,S1,S2,...Sn)を前記記憶領域(10)に記憶させる段階と、オリジナルメッセージに比較してメッセージの完全性をチェックするために、携帯装置の処理回路(11)が、チェックされるべきメッセージの少なくとも一部の少なくとも1つのサインを外部に露見させることなくアルゴリズム(A)を用いて再計算する段階と、該携帯装置の処理回路が、再計算された各サインを、携帯装置の記憶領域(10)に記憶された再計算サインに対応すると予想される各サインに比較し、比較によって一致が得られたか否かを携帯装置外部の手段(2)によってユーザーに示す段階を含むことを特徴とする方法．

2．アルゴリズム(A)が、携帯装置のメモリに記憶すべき各サインを計算するため及びチェックすべきサインを計算するために、その処理回路の制御下にのみアクセス可能な携帯装置の記憶領域(10)に記憶された少なくとも1つのシークレットキー(K)を使用する計算アルゴリズムであることを特徴とする請求項1に記載の方法．

3．記憶すべき少なくとも1つのサインを得るためにオリジナルメッセージの少なくとも一部を計算し且つチェックすべきメッセージを計算するために使用されるキー(K)が、記憶すべきサインの計算を行なう際に決定され、携帯装置のメモリ(10)にサインを導入する際に同時に処理回路(11)の制御下に携帯装置のメモリに導入されることを特徴とする請求項2に記載の方法．

4．サインの記憶の際及びチェックの際に使用されるキー(K)が、携帯装置の処理回路(11)の制御下にのみアク

⑲日本国特許庁(JP)　　⑪特許出願公表

⑫公表特許公報(A)　　平3−503220

㊸公表　平成3年(1991)7月18日

㊿Int.Cl.⁵	識別記号	庁内整理番号
G 06 F 12/14	310 Z	7737−5B
9/06	450 Z	7927−5B
11/10	330 K	9072−5B

審査請求 有
予備審査請求 未請求　　部門(区分) 6(3)

(全15頁)

㊹発明の名称　プログラムまたはデータの完全性をチエツクする方法及び該方法を実施するシステム

㉑特　願　平2−508410
㉒㊱出　願　平2(1990)6月1日
㊲翻訳文提出日　平3(1991)2月6日
㊳国際出願　PCT/FR90/00381
㊴国際公開番号　WO90/15384
㊵国際公開日　平2(1990)12月13日

優先権主張　㉜1989年6月6日㉝フランス(FR)㉛89/07429

㉒発明者　ユゴン，ミツシエル　フランス国、78310・モルパ、リユ・デ・セバージユ、6
㉒発明者　オアゼル，アンドレ　フランス国、78990・エランクール、レ・ヌーボー・オリゾン、5
㉑出願人　ブル・セー・ベー・8　フランス国、78190・トラツブ、リユ・ユジエーヌ・エナフ　(番地なし)
㉔代理人　弁理士　川口　義雄　外4名
㉛指定国　CA,JP,KR,US

請求の範囲

1．コンピュータプログラム及び/またはコンピュータデータの命令のごとき情報を含むメッセージをオリジナルメッセージに対して比較することによって前記メッセージの完全性をチェックするために、処理回路が、オリジナルメッセージ(M)に変換アルゴリズム(A)を適用してサイン(S)を計算するタイアの方法であって、処理回路がメッセージの少なくとも一部を抽出し、アルゴリズム(A)の適用によって前記メッセージ部の関数である少なくとも1つのサインを(S1,S2...Sn)を計算する段階と、処理回路(11)と該処理回路(11)だけがアクセスできる少なくとも1つの非揮発性記憶領域(10)とを内蔵する携帯電子装置をオリジナルメッセージに結合させ、アルゴリズム(A)を実行し得る処理回路の制御下にオリジナルメッセージの各サイン(S,S1,S2...Sn)を前記記憶領域(10)に記憶させる段階と、オリジナルメッセージに比較してメッセージの完全性をチェックするために、携帯装置の処理回路(11)が、チェックされるべきメッセージの少なくとも一部の少なくとも1つのサインを外部に露見させることなくアルゴリズム(A)を用いて再計算する段階と、該携帯装置の処理回路が、再計算された各サインを、携帯装置の記憶領域(10)に記憶された再計算サインに対応すると予想される各サインに比較し、比較によって一致が得られたか否かを携帯装置外部の手段(2)によってユーザーに示す段階を含むことを特徴とする方法．

2．アルゴリズム(A)が、携帯装置のメモリに記憶すべき各サインを計算するため及びチェックすべきサインを計算するために、その処理回路の制御下にのみアクセス可能な携帯装置の記憶領域(10)に記憶された少なくとも1つのシークレットキー(K)を使用する計算アルゴリズムであることを特徴とする請求項1に記載の方法．

3．記憶すべき少なくとも1つのサインを得るためにオリジナルメッセージの少なくとも一部を計算し且つチェックすべきメッセージを計算するために使用されるキー(K)が、記憶すべきサインの計算を行なう際に決定され、携帯装置のメモリ(10)にサインを導入する際に同時に処理回路(11)の制御下に携帯装置のメモリに導入されることを特徴とする請求項2に記載の方法．

4．サインの記憶の際及びチェックの際に使用されるキー(K)が、携帯装置の処理回路(11)の制御下にのみアク

セスできるように製造後に携帯装置のメモリ（10）に導入されることを特徴とする請求項2に記載の方法。

5．携帯装置の記憶領域に記憶させるべく少なくとも1つのサインをオリジナルメモリから計算する段階が、変換アルゴリズム（A）が記憶された携帯装置の回路（11）の外部の回路（2）によって実行されることを特徴とする請求項1から4のいずれか一項に記載の方法。

6．処理回路が完全オリジナルメッセージに変換アルゴリズム（A）を適用して1つのサイン（S）を計算し、チェックの際には、オリジナルメッセージとの比較によってその完全性をチェックすべきメッセージに変換アルゴリズム（A）を適用して1つのサインを計算し、記憶されたサインと再計算されたサインとの一致をチェックすることを特徴とする請求項1から5のいずれか一項に記載の方法。

7．オリジナルメッセージを複数のモジュール（M1,M2,...Mn）に分割し、各モジュールの1つのサイン（S1,S2,...Sn）を計算し、その後のチェックの参照として役立てるために携帯装置のメモリに記憶し、オリジナルメッセージに対するメッセージの完全性をチェックするために、処理回路が、チェックされるべきメッセージ中の所与の数のモジュール（P）を復元し、次いでこれらのモジュール（P）の各々のサインを計算し、このように計算された各サインを、携帯装置のメモリに記憶された対応するモジュールのサインと比較することを特徴とする請求項1から5のいずれか一項に記載の方法。

8．チェックされるべきサインの計算時間が全部のサインのチェックに必要な計算時間よりも短い時間になるように、チェックを行なうモジュールの数（P）がモジュールの総数より少ない数であり、変質を十分な確率で検出できるようにモジュールの総数（m）の関数として選択されることを特徴とする請求項7に記載の方法。

9．サインをチェックしたときに十分な確率で変質が検出されるように、チェックによってカバーされるモジュールの数（P）が、チェックの際に携帯装置の処理回路によって計算されるオリジナルメッセージに内蔵されたモジュールの総数の関数（m）であることを特徴とする請求項7に記載の方法。

10．サインのチェックを行なうモジュールの数を決定するために、携帯装置の処理回路が異なる乱数を（p）回連続して選択し、各乱数がチェックすべきモジュールの数を決定することを特徴とする請求項7から9のいずれか一項に記載の方法。

11．オリジナルメッセージに含まれた（m）個のモジュールからサインのチェックを行なうモジュールの数を決定するために、携帯装置の処理回路が、ビットで表現して長さ（m）の2進数（a）を選択し、選択された乱数の長さがオリジナルメッセージ中のモジュール数を直接示すこと、乱数の値が（m）のうちの（p）のコードから得られること、即ち、乱数中に含まれる（m）個のビット中の（p）個のビットが所定の2進値（1または0）を有し、残りの（m－p）個のビットは補数の値を有すること、乱数の各ビットに異なる通し番号を付け、サインチェックされるべきモジュールの数が乱数中の（m）個のビットから抽出された（p）個のビットの通し番号によって決定されることを特徴とする請求項7から9のいずれか一項に記載の方法。

12．メッセージが、メッセージ中の占有位置に従う通し番号またはアドレスによって検出され得るビットシーケンスから構成され、携帯装置の処理回路によって記憶される前に各モジュールのサインを計算するために処理回路がオリジナルメッセージから種々のモジュール（M1,M2,...Mn）を作成し、各モジュールは、所定のルール及び/または携帯装置の処理回路によって作成されたルールに従っていくつかのメッセージビットを取出すことによって、例えばランダムエレメントを抽出することによって形成され、オリジナルメッセージからモジュールを形成するために使用されたルールと同じルールに従ってチェックされるべきメッセージから該メッセージのモジュールを復元するために、オリジナルメッセージから各モジュールを形成するために使用されたルールが携帯装置に保持されることを特徴とする請求項7から9のいずれか一項に記載の方法。

13．メッセージが2進ワードの形態に構成され、各ワードは、完全性を維持すべきプログラム命令もしくは命令の一部またはデータもしくはデータの一部を形成する所与の数の情報ビットを含み、これらの命令及び/またはデータを用いたプログラムを正しく実行させるために、記憶前に前記命令及び/またはデータのサインを計算し且つ該命令及び/またはデータの少なくともいくつかのサインを計算してメッセージの完全性をチェックするモジュール（M1,M2,...Mn）を形成し、1つのブロックに含まれる各データまたはデータ部が、該当ブロック中での該データまたはデータ

部の構成ビットの位置によって検出されるように、サイン計算を行なう処理回路がまず、各々が所定数のデータを含む所定数（ｎ）のブロック（Ｂ1,Ｂ2,...,Ｂn）を形成し、処理回路が、所与のモジュールを形成するために所与のルールに従って各ブロックから少なくとも１つのビットを抽出することを特徴とする請求項７から12のいずれか一項に記載の方法。

14．ブロックを形成するためにデータをグループ化し、メッセージ読取の際に出現する順序で情報を抽出することを特徴とする請求項13に記載の方法。

15．少なくとも１つのメッセージから少なくとも１つのサインを決定するためにアルゴリズム（Ａ）を実行し得る処理回路（11）を内蔵する少なくとも１つの携帯装置（1）を有すること、更に、所与のメッセージから計算された各サインを記憶する手段（10）と、メッセージを実行し得るコンピュータのごときデバイス（２）への接続手段とを有すること、携帯装置の処理回路が、完全性チェックのために呈示されたメッセージの少なくとも１つのサインを計算しチェック用に計算されたサインとチェック用の再計算サインに対応すると予想される記憶領域に記憶されたサインとを比較するように設計されていること、比較の結果をシステムのユーザーに通知する手段を有することを特徴とする請求項１から14のいずれか一項に記載の方法を実施するシステム。

16．携帯装置（10）のメモリが更に、サイン計算の際にアルゴリズム（Ａ）によって使用されるシークレットキー（Ｋ）を有することを特徴とする請求項15に記載のシステム。

17．携帯装置のメモリ及び/または処理回路が、メッセージから各サインを作成するときのルールを記憶する手段を有することを特徴とする請求項15または16に記載のシステム。

18．複数メッセージに対応するサインが携帯装置のメモリに記憶されていること、及び、携帯装置が、所与のサインが属するオリジナルメッセージを決定する手段を有することを特徴とする請求項15から17のいずれか一項に記載のシステム。

19．プログラムの少なくとも１つのサインが記憶される携帯装置の記憶領域が、携帯装置の処理回路の制御下に書き替え可能なリアログラマブル型であり、メッセージを更新のために意図的に変更する際は、少なくともこの更新後のサインが携帯装置のメモリに記憶されることを特徴とする請求項15から18のいずれか一項に記載のシステム。

明　細　書

プログラムまたはデータの完全性をチェックする方法及び該方法を実施するシステム

本発明は、プログラムまたはデータの完全性をチェックする方法及び該方法を実施するシステムに係る。本発明は、記憶媒体の特定場所に記憶されておりデータ処理システムの毎回の使用毎に一定に維持されるべきデータのごとき情報、または、ソフトウェアとも呼ばれるコンピュータプログラムの動作命令を構成している情報が、連続する使用の間に意図的または偶発的に変更されなかったことをチェックする。実際、プログラムが正しく作動するためには、その命令（または連続する２回の使用の間に必要なデータ）が不正に変更されてはならない。

事実、コンピュータの使用が普及して以来、いかなるユーザーもコンピュータのアプリケーションプログラムまたはオペレーティングシステムにアクセスできるようになっている。

このように広くアクセス可能なため、ユーザーがデータ処理システムの作動に必要なプログラムもしくはデータを変化させる操作エラーを犯したり、または、悪意をもつ人

同がシステムの作動を妨害するためにデータ処理システムのプログラム構造またはデータ内容を故意に改竄することがある．後者の場合には、エラーによって生じた変化よりも問題が難しい．何故なら、意図的な改竄を行なうためには、プログラムまたはデータに命令のような寄生エレメントを導入し、この寄生命令がプログラムによって処理されるときにプログラムが徐々に自己変化するからであり、完全な自己破壊に到達することもあり得る．

更に現在では、たいていのプログラムが複製から保護されており、この保護のために、コピーされた際には、コピーまたはオリジナルを使用の継続に伴って次第に汚染及び/または変質させる手段を含んでいる．このため、ユーザーが海賊コピーを知らずに購入したときに、ソフトウェアが急激に使用できなくなるという問題が生じる．

ソフトウェアまたはデータのこの種のコンタミネーションは、ソフトウェアを徐々に変質させるので、ソフトウェアの誤動作を直ちに生じさせるコンタミネーションよりも検出がはるかに難しい．ソフトウェアの誤動作を直ちに生じさせる後者のタイプのコンタミネーションは一般に異常な処理結果を与えるので速やかに検出される．

これに反して、徐々に変質させるコンタミネーションは、特に悪意をもって与えられたとき、最初の複数回の使用では正しい出力または少なくとも正しく見える出力が与えられるように導入されるので、プリントアウトを読むだけでは必ずしも検出できない．多くの回数の使用後に初めて検出可能なエラーが生じる．

また、最後のタイプのコンタミネーションとして、特にシステムが回線網の一部として使用される場合に、正しいプログラムが実行すべくロードされた後でソフトウェアの正常な動作命令のいくつかに寄生命令を挿入または置換させるものがある．この挿入または置換は、例えば伝送線路を介して遠隔から行なわれる．

この場合、プログラムをロードしたユーザーは、彼がロードしたオリジナルプログラムが正しいことを知っていても外部からの改竄を必ずしも検出できないので、プログラムを実行させると直ちに異常な結果が生じる．

データ処理システムで使用される命令またはデータは、各々が所与のビット数を有する２進ワードの形態でコードされる．常用の１つのフォーマットは、バイト、即ち論理状態「１」または「０」を示し得る８つのビットを含むワードである．命令またはデータのタイプ次第では、１つの命令または１つのデータに複数のワードを使用する必要があろう．プログラムはこれらのワードのシーケンスから成る．前述のごとき変質は、２進ワードの付加、即ち寄生の命令もしくはデータの付加であったり、またはオリジナルプログラム中のいくつかのワードの１つもしくは複数のビットの状態の変化であったりする．

命令またはデータが偶発的に変化した場合に十分に効果的な公知の第１の変質検出方法は、ソフトウェアにサインを付ける方法である．即ち、ソフトウェアまたはデータのサインを構成するために１つまたは複数の２進ワードを命令またはデータに後に付加する．このためには、オリジナルプログラムをメッセージＭとし、Ｓ＝ｆ(Ｍ)で変換し、この結果Ｓをプログラムの所与の場所にサインとして配置する．サインは例えばプログラムの最終ワードから成る．

使用すべきプログラムを後でロードする際にサインをチェックするために、ロードされたプログラムのサインを再計算し、記憶媒体に記憶されているサインと比較する．両者が一致すると、これはオリジナルが変質していないことを意味する．

しかしながら、サインの計算に使用された関数またはアルゴリズムを知っている悪賢いハッカーは、次回の使用の際に、プログラムまたはデータ記憶媒体に記憶されている最新のサインと再計算されたサインとが一致するように、不正侵入の度毎に、記憶させるサインを改竄し得る．従って、サインの一致をチェックする責任者は、メッセージ変換アルゴリズムを用いたときにサインの一致を検出し、改竄を発見できない．

更に、チェックのためのサイン計算は毎回ある程度の時間を要し、しかもこの時間中はプログラムを予定の目的に使用することができない．従って、この方法は長いプログラムには使用し難い．

本発明の目的は、これらの欠点を是正し、すべての状況下に、２回の使用の間でプログラムまたはデータが一致し、意図的であるか否かにかかわりなくプログラムまたはデータが変化しなかったことを高速に且つ確実にチェックし得る方法及びシステムを提供することである．

本発明によれば、プログラム命令のごとき情報またはコンピュータデータのごとき情報を含むメッセージの完全性

をオリジナルメッセージに対して比較することによってチェックする方法が提供される。本発明方法は、該メッセージのサインを処理回路に計算させるタイプの方法である。本発明方法の特徴は、処理回路がメッセージの少なくとも一部を抽出し、処理回路によって実行されるアルゴリズムによって前記メッセージ部の関数として少なくとも1つのサインを作成する段階と、処理回路と該処理回路だけがアクセスできる少なくとも1つの記憶領域とを内蔵する携帯電子装置をオリジナルメッセージに結合させる段階と、先に計算された各サインを該携帯装置の処理回路の制御下に記憶領域に記憶させる段階と、メッセージの完全性をチェックするために、携帯装置の処理回路が、記憶前のサイン計算に用いたアルゴリズム及び記憶後のサインの計算ベースとなったメッセージ部とを用いて少なくとも1つのサインを外部に露見させることなく再計算する段階と、携帯装置の処理回路が、再計算された各サインとこれらに対応する記憶されたサインとを比較し、記憶された各サインとこれらに対応する再計算されたサインとの一致または不一致をユーザーに示す段階とを含むことである。

従って本発明は、プログラムまたはデータの寿命のいかなる時点でも使用できるという利点を有する。実際、自分を守りたいユーザーはいつでも携帯装置内部にサインを記憶させ得る。携帯装置は好ましくは、電子マイクロ回路を備えたメモリカード型のデバイスである。設計者がサインを記憶させてもよい。その場合には、携帯装置にプログラムが導入されている。また、多数回の使用後にプログラムが無傷（intact）であることをチェックしたいユーザーがサインを記憶させてもよい。その場合には、ユーザーは特定のバージン携帯装置を入手し、必要なときにサイン計算プログラムを実行させてサインを記憶させる。次いでこの携帯装置を使用してプログラムの完全性をときどきチェックする。

更に、最初に記憶されたサインに比較するためのサインが携帯装置の内部で計算され、携帯装置の処理回路だけがアクセスできる記憶領域に記憶されたサインを抽出することによってサインの一致がチェックされるので、ハッカーがシステムを破壊することは不可能である。何故なら、各サインは、携帯装置の回路によって再計算され、処理回路の制御下でのみアクセス可能な比較回路に送られるからである。従って、メッセージが無傷でないときは、比較回路のアドレスに偽サインを送ることはできないので、いかなる改変または侵入も直ちに検出される。

1つの実施態様によれば、記憶すべきサインの計算に必要なシークレットキーが、これらのサインを作成するときに使用され、計算された各サインと同様に携帯装置のメモリに記憶される。シークレットキーは、サイン計算の際に与えられ、計算後に携帯装置に記憶された後で破壊される乱数でよい。

1つの実施態様によれば、記憶させるサインの計算に使用されるシークレットキーが、携帯装置の内部、例えばその機密フェーズに予め記憶され、携帯装置の外部からアクセスできない。携帯装置自体の処理回路が、予め記憶された前記キーを用い、記憶すべきサインの最初の計算を実行する。

本発明のその他の特徴及び利点は、本発明の原理及び本発明のいくつかの実施例を示す添付の図1から図6に基づく以下の記載より明らかであろう。

図1Aから図1Dは、本発明が適用される情報シーケンスのそれ自体公知の構造を示す。

図1Aは、プログラムの典型的構造を示す。プログラムは、夫々のアドレスによって検出され得るワードによって2進形にコードされ1からkまで番号付けされた一連の命令から構成されている。図示の実施例において、プログラムはm個の2進ワードを有し、mはk以上の値でよい。命令のタイプ次第では、1つの命令のコードが複数の2進ワードに関係する。このことが図1Aに示されている。この図において、命令No.2は2つのワード、即ちワード2及び3にコードされている。構造化データ処理システムにおいては一般に各ワードが所与のビット数を有し、通常はバイト、即ち8ビットのサイズを有するかまたは8ビットバイトの倍数のサイズを有する。勿論、本発明はこのプログラム構造に限定されるものではなく、ワードフォーマットが個々のプログラム毎に異なった他のいかなるプログラム構造にも適用できる。

このように構造化されたプログラムは、同じ長さ、即ちnビットのワードを有し、これらのワードが所与の順序で配列されると、ビット数で表現して合計長さL＝m×nのメッセージを構成する。一般に、メッセージの合計長さは、命令シーケンスに使用された各ワードを構成するビット集合の和から成る。

本発明はまた、図1Bに示すようなデータシーケンスの完全性をチェックするために使用される。繰返し使用されるデータ、例えばプログラムの実行に必要なデータの完全性をチェックすることが必要になることもあろう。

データは、図1Bに示すようにプログラムから独立していてもよい。図1Bは、J個のデータを含むm個のnビットワードの集合を示す。

データは命令と同様に、複数の2進ワードでコードされ得る。従って、データ数Jがデータを含むワード数mとは異なる値になり、Jがm以下になり得ることは理解されよう。

図1Cは命令とデータとが混合されたプログラム（x個のデータとy個の命令）の特定例を示す。

一般に、命令はデータの特定形態であると考えられることに注目されたい。

プログラムは通常、特定記憶媒体、例えばコンピュータのＣＰＵまたはマイクロコンピュータプログラムを内蔵したハードディスクに記憶される。プログラムはまた、最初に記憶されたディスケットのようなオリジナル記憶媒体から直接使用されてもよい。意図的であるか偶発的であるかにかかわりなくプログラムの完全性が欠如したとき、その結果として上記のごときワードのいずれかが変化する。

図1Dは、実際に「0」または「1」の値をとるビットの集合からワードが構成されることを示す。1つのワードが変化すると、その結果として少なくとも1つのビットの状態が変化する。または、オリジナルの命令またはデータに寄生の命令またはデータが重畳されたときにも変化が生じる。これは、オリジナル記憶媒体以外の媒体にプログラムを記憶させるとき、例えばプログラムをオリジナルハードディスクから使用ハードディスクに記憶させるときに生じ得る。

従って、寄生即ち改変された命令またはデータが読取られたときは制御不能な現象が発生し得る。

本発明はプログラム及び/またはデータの完全性をチェックするために使用されるので、本発明では、以上の記載で命令もしくはデータと呼びまたは情報と呼んできたシーケンスがビットで表現して長さしのメッセージを構成し、Lの値がメッセージ中のビット数に等しいと考えている。

小サイズのメッセージに直接使用される第1の方法は、少なくとも1つのシークレットキーを用いたメッセージ変換アルゴリズムＡを使用してメッセージの電子サインを予め計算し、次いで、得られたサインＳを、サインを予め計算する際に使用したアルゴリズムを有するマイクロコンピュータカードの電子メモリに記憶させる段階を含む。携帯装置は更に、該装置が内蔵する処理回路だけがアクセスできる記憶領域を有し、任意に、サインを予め計算する際にシークレットキーを使用したときは該シークレットキーを含む。

メッセージの完全性をチェックする際に、ユーザーが携帯装置をプログラム内蔵システムに接続し、チェックプログラムを実行させる。このチェックプログラムでは、携帯装置の処理回路がその内蔵アルゴリズム及び任意にシークレットキーを用いてチェックされるべきメッセージを構成するビットシーケンスに関する別のサインを再計算する。

次いで、携帯装置の処理回路を使用し、再計算されたサインを、最初に計算され携帯装置の処理回路だけがアクセスできる携帯装置のメモリに記憶されたサインに比較する。最初のサインの計算のベースとして使用されたメッセージがチェックに使用されたメッセージに等しいとき、即ち、プログラム及び/またはデータが変質していないときは、携帯装置のメモリに記憶されたサインは再計算されたサインに等しく、このことがチェック担当者に示されるであろう。

本発明の別の利点も容易に理解されよう。チェック用サインが携帯装置の処理回路によって計算され同じ処理回路によって携帯装置の内部で比較されるので、偽サインをシミュレートすることは不可能である。その理由は、ハッカーが改変プログラムまたはデータに対応する偽サインをプログラム及び/またはデータに結合できた従来技術の場合と違って、処理回路が偽サインを抽出しないからである。

図2は、携帯装置のメモリに記憶されるチェック用サインをシークレットキーＫを用いて計算する本発明の実施例の原理を示す。

長さしのメッセージＭを、例えば単位ブロックB1,B2,...,Bfに分割する。各単位ブロックは、サイン計算を実行する処理回路のワーキングフォーマットとコンパチブルなビット数を含む。例えば各ブロックが1ビットを含んでもよいが、最新の処理回路では、各ブロックがバイトの倍数から成る複数ビットから構成される。第1ブロックB1は例えば、サイン用ベースとして機能するメッセージの第1ワードから成り、第2ブロックB2はメッセージの第2ワードから成

り、以後同様にして最終ブロックBfはメッセージの最終ワードから成る。複数のワードまたは各ワードの複数ビットを、記憶媒体での記憶順序とは異なる順序で抽出する計算アルゴリズムを使用するのでハッカーの作業は勿論複雑になるであろう。

この原理は、メッセージを構成するビットの数が回路処理フォーマットに対応するビットの数よりも明らかに多いのに、携帯装置の処理回路によって直接使用され得るフォーマットを有するサインを計算することにある。

図２で示した原理は、ブロックと同数のオペレーションを実行し、限定数（ｓ）のビットを有するサインＳを得るために各オペレーションの結果を総合することにある。アルゴリズムＡを使用して処理回路の入力に初期値VIを与え、同じ回路の別の入力にシークレットキーＫを与え、シークレットキーＫと初期値VIとの適用によって第１中間結果を作成し、これを例えばEXCLUSIVE OR関数を介して第１ブロックB1の内容と総合する。EXCLUSIVE ORを介して得られた変換の結果を、アルゴリズムを用いる処理回路の第１入力に与え、第２入力にシークレットキーＫを与え、処理回路の出力に第２の中間結果を得る。これを同じ変換関数、即ちEXCLUSIVE ORを介して第２ブロックB2の内容と総合する。

最終ブロックBfまで各ブロックを順次同様に処理し、最終ブロックの内容を、EXCLUSIVE OR関数を介して、それまでの結果Rfと合わせる。結果Rfは、処理回路にアルゴリズムＡとシークレットキーＫとを適用し、それまでのEXCLUSIVE ORの結果を合わせて得られたものである。ブロックBfの内容とそれまでの結果RfとにEXCLUSIVE ORを適用して得られた結果を、サイン計算回路のアルゴリズムＡを介してキーＫと総合し、この総合結果がサインＳを構成する。

勿論、チェックのためには、初期値VIは最終計算に使用される初期値と同じでなければならない。

サインＳの計算が終わったとき、サインＳは以後のチェックで参照として使用できるように携帯装置のメモリに記憶される。メッセージを使用する前にメッセージの完全性をチェックする必要があるときは、携帯装置は、計算されたサインが携帯装置のメモリ内で処理回路だけがアクセスできるように記憶されたサインと真に同じサインであることをチェックするだけでよい。

初期値VIは、携帯装置に内蔵された値、例えばその通し番号から構成されてもよい。また、記憶させるべきサインの計算を開始する人間によって入力されメッセージの完全性のチェックを要する別のユーザーに与えられた機密コードであってもよい。最後に、初期値VIは、携帯装置の特定の記憶レジスタの内容であってもよい。この内容は携帯装置の毎回の使用で等しい。値VIはまた、記憶前にサインを計算するときに処理回路によって決定されサインと同時に記憶される乱数であってもよい。

図２に示す実施例は１つの例にすぎない。アルゴリズムを異なる方法で使用することも勿論可能である。また、初期値及びシークレットキーＫを使用しなくてもよい。また、EXCLUSIVE OR関数以外の関数を使用してもよい。

メッセージの完全性をチェックするための携帯装置のメモリは少なくとも１つの信号Ｓを含み、携帯装置はまた、プロセッサのごとき処理回路と変換アルゴリズムＡとを有する。携帯装置は、チェックされるべきメッセージが携帯装置の処理回路に送られるように設計されている。携帯装置はまた、シークレットキーＫを含んでもよく、この場合、サインは計算の結果である。

図３は、携帯装置の処理回路11だけがアクセスできる非揮発性記憶領域10に複数のサインS1,S2,...Snと１つのシークレットキーＫとを含む改良された携帯装置１の例を示す。各サインは実際、異なるメッセージのサインであり、同じシークレットキーＫから得られたものである。この構成（configuration）は、１つのソフトウェア業者が同一ユーザーに複数のプログラムを提供するときに使用される構成である。この場合、各プログラムのサインは同じ携帯装置に記憶され得る。

更に、アルゴリズムＡは装置の別の記憶領域12に記憶されている。

これは、保護を望むユーザーがシークレットキーＫを最初から含む特殊な携帯装置を使用し、該ユーザーが所有する各プログラム及び/またはデータ記憶媒体のサインを該携帯装置に記憶させる場合に適している。

かかる場合、即ち、１つの携帯装置が複数のメッセージのサインを含む場合には、サインをチェックする際に、携帯装置の処理回路が、チェックされるメッセージに一致すると想定されるオリジナルメッセージのサインをメモリ内で検索できるように、各サインをオリジナルメッセージの識別手段に結合させる必要がある。このために、記憶させるべきサインを予め計算する際に、各オリジナルメッセー

ジに通し番号または別の識別子を付加する．この通し番号または識別子に対応するデータは対応するサインを記憶するときに携帯装置に記憶され、従って携帯装置の処理回路は、識別データと対応サインとを相関させ得る．

通し番号、または識別子は、記憶させるべきサインを予め計算することを望むユーザーによって決定されてもよく、または携帯装置自体の処理回路によって決定されてもよい．

携帯装置を単独で使用しないことも勿論可能である．その場合、後述するすべての変形例と同様に、結合及び/またはインタフェース回路によってより大きいシステム２．特に、オリジナルメッセージ（プログラムまたはデータ）を処理するデータ処理システムと結合させる必要がある．このデータ処理システムは一般にコンピュータの一部であり、少なくとも１つのキーボードとプリント及び/またはディスプレイ手段とを有する．結合及び/またはインタフェース回路は、携帯装置の処理回路とより大きいシステムの処理回路との間に対話を成立させ得る．

プログラムの通し番号または識別子を決定するのがユーザーである場合、ユーザーはこれらを例えばより大きい処理システムのキーボードを介してシステムに入力する．これに反して、対応するデータを決定するのが携帯装置の処理回路である場合は、オリジナルメッセージ（そのサインはユーザーによって予め計算されている）に付加された通し番号または識別子が、携帯装置の処理回路とより大きいシステムの処理回路との間に対話が成立した後で、該システムのディスプレイ手段またはプリント手段によってユーザーに通知される．

どの変形例を使用するかにかかわりなくユーザーは、所与のオリジナルメッセージに対応する識別子または通し番号の記録を種々の記憶媒体に保持し、チェック用サインを計算する際にキーボードまたはその他のデータ入力手段を使用して該サインをシステムに通知し、携帯装置の処理回路が、対応すると想定されるメモリ内のサインだけにサインを比較する必要がある．

記憶させるべきサインの計算は、携帯装置のメモリ回路10において、携帯装置自体の処理回路11と製造後に任意に該回路に組込まれたシークレットキーとから直接実行されてもよい．この計算方法は、処理回路が計算を終了すると直ちにサインを記憶するので、決して外部に露見させずにサインを計算できるという優れた利点がある．または、記憶される前の最初のサインの計算が、携帯装置１と接続され得る外部システム２に組込まれた携帯装置外部の処理回路によって実行されてもよい．外部システム２は例えば、チェックすべきプログラムまたはデータの処理装置である．これらの外部回路は、携帯装置に内蔵されたアルゴリズムと同じアルゴリズムを使用する．かかる場合、計算にシークレットキーを使用するときは、シークレットキーは、各サインを計算し記憶するときに同時に決定されてもよく、または、携帯装置が内蔵する処理回路の制御下に携帯装置の内部から抽出され、次いで記憶すべきサインを計算するために外部回路に伝送されてもよい．この方法には、シークレットキーを外部に伝送しなければならない、その結果として、サインの計算後にシークレットキーを外部処理回路から抹消しなければならないという欠点がある．しかしながらこの方法は、プログラムが極めて長いのでサインの計算にかなり長時間を必要とする場合には有利である．サインの計算がプログラム及び/またはデータを構成するメッセージ全部に基づいて行なわれる限り、マイクロプロセッサＣＰＵの処理時間は方法の使用に対する障害となる．実際、１メガバイトのプログラムの場合、サイン計算の結果を得るため、従ってチェックの結果を得るために１時間以上の計算時間を要する．その理由は、マイクロ回路カードのような常用の携帯装置に組込まれた処理回路は、処理時間に関しては、より強力なコンピュータよりも明らかに劣っているからである．

チェック処理時間が長いと頻繁な使用には全く不適である．このような理由から別の変形例では、同様となるすべての場合に使用でき前述の方法よりもはるかに高速なチェック方法を提案する．ここではメッセージがいくつかの部分即ちモジュールM1,M2,....Mnに予め分割され、サインS1,S2,...Snが各モジュールに付加され、各サインは携帯装置の異なる機密領域に記憶されている．記憶の前にそのサインS1,S2,...Snを計算する必要があるメッセージのサイズ次第で、メッセージが余り長くない場合には携帯装置の処理回路によって計算を実行し、極めて長時間の計算を要するサイズであるときは、より高速の処理回路、例えばサイン計算フェーズで携帯装置を接続させるコンピュータの処理回路で計算を実行する．

しかしながら、携帯装置のメモリ10にサインを記憶させるべくサイン計算フェーズ中の計算時間は最重要条件では

ない．従ってシークレットキーが外部に露見することを防止することを重要視するならば，携帯装置自体の処理回路11によって計算を実行するほうが好ましいことは理解されよう．

1つのメッセージ全体が複数のサインを作成するためのベースとして使用され，従って，メッセージを構成する全部のビットが用いられたことが理解されよう．かかる場合，複数のサインの作成のベースとなったメッセージの完全性をチェックするためにいくつかの方法を使用し得る．

第1の方法では，チェックすべき完全プログラムを示すm個のモジュールの集合から異なる複数のp個のモジュールをランダムに選択する．数pは所定の値であり，各チェック毎に一定である．処理回路は1回のチェックに異なる複数のモジュールを選択し，毎回のチェック毎に異なるモジュールを任意に選択できるように設計されている．

モジュールを決定するために，携帯装置の処理回路は，m個のサインの初期計算に使用されたm個のモジュールを決定した手続きと同じ手続きを使用する．従って，初期計算の際にメッセージがkビットのモジュールに分割されたならば，サインチェックの際にも携帯装置の処理回路は，受信メッセージをkビットのモジュールに再度分割し，これらのモジュールからサインチェック用のp個のモジュールをランダムに選択する．携帯装置の処理回路は次に，選択されたp個のモジュールのサインを計算し，これらをカードのメモリ内の対応すると想定されるサインに比較する．

比較は即座に行なわれてもよい．即ち，カードがサインを再計算したとき，このサインが，該サインに対応すると想定されるメモリ内のサインに一致するか否かが直ちにチェックされてもよい．または，再計算されたサインをバッファメモリに記憶し，p個のサインの再計算の終了後に比較を行なってもよい．

携帯装置の処理回路が，再計算されたサインとこれに対応すると想定される携帯装置のメモリ内のサインとの不一致を検出すると直ちに，メッセージが無傷でないと判断され，処理回路に結合した手段，例えば携帯装置に接続されたシステムのディスプレイ手段が，比較の肯定または否定の結果を表示する．

従って，例えば，オリジナルメッセージが8ビットモジュールに分割されたとき，第1モジュールはメッセージの最初の8ビットから成り，第2モジュールは次の8ビットから成り，以後同様である．第1モジュールの記憶されたサインは，最初の8ビットの計算に対応し，第2モジュールのサインは，オリジナルメッセージの9番目から16番目のビットの計算に対応する．サインチェックの際に処理回路が，第2モジュールのサインをチェックすると決定したならば，処理回路は，完全性をチェックすべきメッセージの2番目の8ビット集合を抽出し，チェックすべきメッセージのこの2番目の8ビット集合のサインを再計算し，この8ビット集合にアルゴリズムAを適用し，必要な場合には記憶前の計算で使用したシークレットキーKを適用し，携帯装置のメモリに記憶された第2のオリジナルモジュールに対応するサインを，これに対応すると想定されるモジュールの再計算されたサインに比較する．

勿論，再計算されたp個のサインが正しいとき，最初に計算され携帯装置のメモリに記憶されたm個のサインがチェックされなくても，システムは，プログラムが無傷であると判断し，比較の肯定結果を表示する．

携帯装置によってチェックされるべきモジュールの数pは所定の数でもよく，チェックされるモジュールは毎回のチェック毎に異なっていてもよい．チェックされるべきモジュールの数pは，携帯装置の処理回路に表示され，許容信頼度水準を得るために十分な徹底チェックが行なわれるように選択される．最初のm個のサインの代わりにp個のサインがチェックされるので，チェック用計算の所要時間は全部のサインの記憶に必要な計算時間に比べてかなり短縮される．

また，計算されるモジュール数pを前以て決定せず，携帯装置の処理回路によってランダムに選択してもよい．この場合，チェックがカバーするモジュールの数が少なすぎてチェックの妥当性が不十分にならないようにpの値を選択する必要がある．また，処理時間を許容限度内に維持するために数pが多すぎないようにする必要もある．

図4は，0.9の確率Prを得るためにチェックすべきモジュール数pを，メッセージが含むモジュール総数mの関数として示すグラフである．即ち，このグラフは，メッセージがp個のチェック済みモジュールに等価のq個の変質モジュールを含む場合，メッセージ変質を9/10の確率で検出したいときにチェックすべきモジュールの数を示す．例えば，約60個の変質モジュールを含む1000個のモジュールを含むプログラムにおいては，メッセージ変質を9/10の確率で検

出するためには60個のモジュールをチェックする必要がある．

言い替えると、1000個のモジュールを含み60個未満の変質モジュールを含むメッセージにおいて約60個のモジュールのサインをチェックすると、この60個のモジュールのサインチェック後の変質検出確率は9/10以上であり、検出確率は変質モジュール数の増加に伴って低下する．

従って、チェックを要するモジュールの数pを決定するためには、変質モジュールの数qとメッセージに含まれるモジュールの総数nとの間で妥当値を調整する．

前述のごとく各モジュールが通し番号で見付けられると仮定すると、サインチェックを行なうべきp個のモジュールのランダムな選択は、携帯装置の処理回路に異なるp個の乱数を生成させることによって得られる．乱数の各々が選択されたモジュールの通し番号を決定する．

従って、m個のモジュールの集合に4回のチェックが必要であると仮定すると、携帯装置の処理回路は4つの異なるm以下の数をランダムに抽出する．例えば、計算によって数2，4，j，m－1が与えられると、携帯装置の処理回路は、その完全性をチェックすべきメッセージの2番目、4番目、j番目及びm－1番目のモジュールのサインを計算し、これらを携帯装置のメモリに記憶された2番目、4番目、j番目及びm－1番目のサインに比較する．

比較後に、携帯装置の処理回路は、種々の比較において不一致が検出されたか一致が検出されたかを示す手段を作動させる．

1つの変形例においては、どのモジュールでサインチェックを行なうべきかを決定するために、携帯装置の処理回路は長さmの2進数、即ちメッセージを構成するモジュール数に等しいビット数を有する2進数（a）を計算する．2進数はmビット中のpビットのコードから得られる．即ち、p個のビットが所与の論理状態であり、残りのm－p個のビットは補数の論理状態である．例えば、ビットの初期状態が論理状態「0」の場合、数（a）の発生によってp個のビットは残りのビットの状態とは異なる状態になる．各ビットがmビット集合中の通し番号によって検出できるので、サインチェック用に選択されたモジュールは、ランダム2進数（a）中で「1」に変化したビットの通し番号に対応する通し番号をもつモジュールであろう．

本発明の範囲内でその他の変形も可能であることが当業者に理解されよう．

前述のいくつかの実施例は、メッセージの変質の有無を優れた確率で判定し、適正且つ十分に高度な信頼性を与える．しかしながら、方法の信頼性を更に向上させるその他の変形例も可能であろう．

これらの改良例は、改竄が一般にプログラム中の逐次命令のシーケンスの変更、またはかなり局在し且つ組織には使用されない寄生シーケンスの導入から成ることに基づく．プログラム実行の際に寄生命令が使用されたときに始めてその存在が有害であることが判明する．これらの寄生命令はある種の使用条件下ではプログラムによって呼び出されないがその他の条件下では呼び出される．

このような理由から、使用されることの少ない極めて局部的な変質の検出確率を改良するために、1つの変形例では、サイン計算に先立って携帯装置の処理回路で使用されるアルゴリズムは、メッセージをその内容にかかわりなくブロックに分割するように編成され、メッセージの首尾一貫した変質が不可能になるようにサイン計算中にブロックの組み合わせを編成する．このような組み合わせたブロックの集合がモジュールを形成する．

従って、メッセージを構成する1つの2進ワードの各々が1つのブロックを構成する場合を考察する．かかる場合、処理回路のワーキングフォーマットがバイトの場合、各ブロックは8ビットから構成されるであろう．

1つの変形例では、1つのブロックが、1つの2進ワードから構成されるのでなく例えばメッセージのシーケンス中の連続する複数の2進ワードから構成されると考えられる．従って、第1ブロックは、例えば最初の100個の2進ワード、即ち完全性をチェックすべきメッセージの最初の100ワードから成り、各ワードは所与の数のビット、例えば8もしくは16ビットを有するかまたは携帯装置の処理回路のワーキングフォーマットとコンパチブルなその他のビット数を有する．第2ブロックは次の100個の2進ワードから成り、メッセージの終端まで以後同様である．

勿論、メッセージ中のワードの総数次第では、最終ブロックが、メッセージに属する先行ブロックと同数の2進ワードから構成されない場合もある．この場合には、メッセージ中のワードの総数を各ブロックを構成するワード数によって除算した商が整数でない．このような場合、最終ブロックは、メッセージ中の先行ブロックに含まれるワード数と

同数のワードを含むことができない。

例えば、1つのメッセージが1030ワードを含み各ブロックが100ワードから成る場合を考える。100ワードのブロックが10個形成され、最終ブロックを形成するために30ワードだけが残る。この場合、最終ブロックは、この残りの30ワードに、例えば2進値0の70ワード、即ちすべて0から成る70ワードを付加することによって形成される。

上記のごとき方策を用いる必要をなくすために、各ブロックのワード数がメッセージ中のワード数の完全な約数であり、ブロック集合がオリジナルメッセージのワードだけを含むようにすることができる。この解決では、処理回路が1ブロック当たり何ワードにするかを決定するために、ブロックを形成する前にメッセージ中のワードの総数をカウントしなければならないという欠点はある。従って、処理回路が各ブロック中の最適ワード数を予め知っていることが必要であり、この最適数がメッセージ中のワードの総数の約数でないときは、処理回路は、使用できるより小さい約数を決定しなければならない。従ってこの解決は、可能ではあるが、多少面倒で実行が難しい。

図5は、メッセージ内部でブロックがどのように分割されるか、及び、処理回路が最初のサインをどのように計算するか、または、携帯装置の処理回路がチェック計算を実行するときにどのようにサインを組み合わせるかを示す。

図5には、m個のブロックb1～bmの集合が示されている。各ブロックは前述のように、1つの2進ワードから成ってもよくまたは互いに結合した複数の2進ワードから成ってもよい。所定数のブロックを互いに結合させることによって、前述のごとくサインの計算のベースとなる1つのモジュールが得られる。

メッセージPをm個のブロックB1～Bmに分割すると、n個のブロックから成るモジュールがm/n個得られる。各モジュールは、ランク1のモジュールHiが、ランクi, i+1, i+2nのブロックから成り、以後同様にしてi+rnまで続く。但し、$1 \leq i \leq n$及び$0 \leq r \leq m/n-1$である。

従って、最初のモジュールは互いに隣接するブロックB1, B1+n, B1+2n, ...B1+rnから成る。

数nは、サイン計算及びチェック時間が余り長くならないように且つ各モジュールができるだけオリジナルメッセージ即ちチェックすべきメッセージからの情報だけを含むように決定する必要がある。

nがブロック数の完全な約数でないとき、いくつかのモジュールは、サインを計算すべきメッセージの情報以外の情報を含むことになる。実際、いくつかのモジュールに2進数0または1を補充する必要があったからである。

このため、各モジュールのブロック数nは、nがメッセージ中のブロックの総数の約数になるように選択されるのが好ましい。

各ブロックのワード数及び各モジュールのブロック数にかかわりなく、モジュール中のブロックの相互結合及びサインはメッセージの情報自体には全く無関係である。これは、メッセージがその完全性をチェックすべきプログラムである場合には特に重要である。実際、この相互結合によってメッセージの一部の変質がいくつかのサインに出現する可能性があり、その結果として、いくつかのモジュールが初期状態に比べて変化を生じ易くなるので変質の検出確率が高くなる。いわば、変質が、モジュール全体または少なくない数のモジュールに拡散する。従って、各モジュールがメッセージ中で直列に連続する所定数のブロックから成る構成に比べて、この構成では、サインチェックのための計算回数を減少させ得る。

図6に示すモジュールの別の形成方法では、前記方法と同様に、全メッセージを各々が所与の数のビットまたはワードを有するブロックB1, B2, B3, ...Bmに分割する。例えばブロックB1は、メッセージの最初のk個の2進ワードから成り、ブロックB2は次のk個のワードから成り、以後同様にして終端まで続く。この場合にも、数kは、例えばメッセージ中のワード数の約数であり、携帯装置に記憶される前のサイン計算のための構成の際に形成される最終ワードがオリジナルメッセージに属するワードだけから成り従ってブロックに無効情報を補充する必要がないように選択される。

従って、各ブロックは所与の数のビットを有し、各ビットは、ブロック中のランクによって検出できる。モジュールの形成は、ブロック中の所与のランクの1つまたは複数のビットを別のブロック中の同じランクの1つまたは複数のビットと組み合わせることによって行なわれる。次に、このように形成されたモジュールを使用してサインを計算する。

従って、各ブロックから1ビットを抽出してモジュール

を形成すると仮定すると、第１モジュールは、メッセージ中の第１ブロックの第１ビットと、第２ブロックの第１ビットと、同様に以後のブロックの第１ビットと、最終ブロックの第１ビットから形成される。第２モジュールは、第１ブロックの第２ビット、第２ブロックの第２ビット、などから形成される。

従って各モジュールは、考察中のメッセージと交差する情報ストリングから構成される。その結果、サイン再計算の際に、再計算され出発サイン数に比較されるサイン数にかかわりなく、メッセージの一部の首尾一貫した変質が検出されずにすむことは極めて難しい。一般に、プログラムであるかデータにあるかにかかわりなく命令は、長手方向に連続して書込まれ、プログラムまたはデータ中に最小限の首尾一貫した変質が生じても、異なるクロスストリングを同時に処理することがほぼ不可能になる。更に、この解決では、メッセージをチェックする際に再計算して対応するオリジナルサインに比較すべきサインの数を減少させ得る。

また上記のごときクロスストリングを選択しないで、記憶する前に各サインを計算するときに所与の数のビットを各ブロックからランダムに抽出してモジュールを疑似クロスストリングから形成してもよい。例えば、第１ブロックから第１ビットを抽出し、これを第２ブロックの最終ビットと組み合わせ、次いで第３ブロックの異なるランクのビットと組み合わせることが可能である。勿論、かかる組み合わせには、例えば記憶前のサイン計算の際に選択された参照乱数を使用する必要がある。この参照乱数は、どのビットシーケンスを考察すべきを決定するために処理回路によって使用され、また、チェックの際に処理回路がチェックすべきメッセージからモジュールを形成するためにどのような分布を用いるべきかを知ることができるように、携帯装置のメモリ回路に記憶されなければならない。

更に、モジュールを形成するためのブロックの組み合わせまたはブロックを形成するためのワードもしくはビットの組み合わせの変形を考えることが可能である。特に、ワードまたはブロックの互いの組み合わせを論理的シーケンスに従って形成する代わりに、ブロックを形成するワードの組み合わせまたはモジュールを形成するブロックの組み合わせをランダムに行なってもよい。このためには例えば、処理回路が記憶用サインを計算するためにモジュールを形成する前に、モジュールの復元方法を決定し、後でチェックできるようにモジュール形成に使用されたパラメータを記憶する必要がある。例えば、処理回路にｎ個の乱数のシーケンスを作成させることが考えられる。ｎは各モジュールのブロック数に対応する。メッセージはｍ個のモジュールを含む。乱数V1,V2,V3,...Vnのシーケンスは、モジュールの第１ブロックを構成するブロックからこのモジュールの別の構成ブロックがどれであるかを判断できる。

この場合、チェックすべきメッセージからモジュールを復元できるように、使用した乱数シーケンスの記録を保持する必要がある。

チェックの機密を保持するためにはシークレットキーの使用が好ましいが、キーを使用する必要がない場合、即ちメッセージをモジュールに分割するかまたは分割しないで１つまたは複数の明確なサインの作成に使用できる場合もある。しかしながら、各携帯装置は異なるシークレットキーを含むので、シークレットキーの使用は、同一メッセージ中のサインの計算に使用される異なる２つの携帯装置が等しいサインを含むことを防止し、機密保持を向上させる。このため、ハッカーがプログラムのごときメッセージで行なわれていることを観察しサインチェック手段を破壊することを試みた場合にも、改竄の危険が少なくなる。特に、例えばプログラムを１個人から別の個人に転送するときにシークレットキーの使用が重要である。しかしながら最終ユーザーが、後でチェックすべく記憶するためにメッセージの１つまたは複数のサインの計算を必要とする場合、チェックに使用される携帯装置がシークレットキーを必ずしも含む必要はない。メッセージのサインは、メッセージが含むデータを全体または別々のモジュールとして抽出し、アルゴリズムを用いて変換するだけで得られる。従って各サインは、その計算に使用されたデータの簡単なピクチャである。最終ユーザーがその使用中にデータ記憶媒体の完全性をチェックしたい場合、これはシステム破壊の企てとは全く関係がない。かかる場合、サインは情報の単なる圧縮によって得られる。

メッセージまたはメッセージの一部に関するサインの計算は、該当するアルゴリズムで処理したメッセージまたはメッセージの一部だけの関数であろう。

従ってサインチェックのためにサインを計算する携帯装置は、図３の場合のようにシークレットキーＫを組込んだ

記憶領域10をもはや含まず、逆に、各々がサインS1,S2,Snを含む1つ以上の記憶域を含み、同時に、アルゴリズムAを実行する処理回路11を備えたプロセッサを含むであろう。

その結果として、図2に関して説明したようなサインの作成は、サイン計算に必要な各中間処理の際にシークレットキーKを使用しないで行なわれる。

本発明を実行するためのシステムは、プログラムの少なくとも1つのサインを記憶する少なくとも1つの記憶領域10と、少なくとも1つのオリジナルサインの書込み後に少なくともサインを再計算するためにアルゴリズムAを記憶している処理回路11とを有する携帯装置1を含む。例えば計算時間が長くなることを避けるために携帯装置のメモリに記憶されたサインが携帯装置の外部の処理回路で計算されたとき、外部オブザーバーがこの最初に計算されたサインを知っていたとしても、再計算が携帯装置の処理回路の内部で行なわれるので、外部オブザーバーは、再計算されたサインの値を知ることができない。

従って、携帯装置の処理回路は、完全性をチェックすべきメッセージMを少なくとも変換するためのアルゴリズムまたは計算プログラムAを含んでおり、更に高度な機密保持を要するときはメモリがキーKを含み得る。更に、携帯装置のメモリが、オリジナルメッセージの異なるモジュールに各々が所属する多数のサインを含む場合には、携帯装置の処理回路は、計算時間を短縮するために初期数よりも少ない数のモジュールのチェックを実行するように構成されるのが好都合である。また、処理回路は、チェックすべきメッセージのモジュールをサインが計算され記憶されたときと同様の構成に復元できるようになっていなければならない。

勿論、サインが記憶された記憶領域は非揮発性記憶領域である。

また、上述のごとく、携帯装置1は単独では機能できず、本発明方法を実行するシステムを構成するために別の手段2と組み合わせる必要がある。特に、携帯装置とコンピュータとの間、またはその完全性をチェックすべきプログラムまたはデータの処理装置との間にインタフェース回路を構成しなければならない。この処理装置またはコンピュータを介して、チェックすべき情報は、オリジナルメッセージを構成する情報と同様に、携帯装置の処理回路に結合した処理装置の処理回路との対話後に携帯装置内で処理される。特に、処理装置に通常存在するキーボードまたはその他のデータ入力手段（マウス、タッチスクリーンなど）を使用して、特に機密アクセスキーまたはオリジナルメッセージに対してその完全性がチェックされるメッセージに対応する識別子を入力するときに携帯装置との対話を成立させる。

インタフェース回路は、処理装置またはコンピュータに直接組込まれてもよくまたは外部に設置されリンクで接続されてもよい。勿論、携帯装置とインタフェースまたは結合回路との間にコネクタが配備される。

システムをチェックに使用するとき、オリジナルメッセージを完全にカバーする1つのサインが記憶されている場合には、携帯装置の処理回路は完全性をチェックすべきメッセージ全体を検出し、内底するアルゴリズムを使用してこのメッセージのサインを計算し、再計算されたサインが記憶されたサインに一致するか否かをチェックする。これは短いメッセージに適している。

しかしながら、オリジナルメッセージが比較的長いので複数のモジュールに分割し、その結果として携帯装置のメモリに複数のサインが記憶されているときは、携帯装置の処理回路は、サインチェックすべきモジュールの数pとその通し番号とが予め決定されていないときはこれらを決定する。全部のサインを予め計算する際にオリジナルメッセージ中の対応すると考えられるモジュールが構成されたときと同様に、この通し番号を用いてサインチェックすべきモジュールを復元する。

好ましくは、メッセージのどの部分をチェック用サインの計算に使用したかをハッカーが突き止めることを防止するために、携帯装置の処理回路が全部のメッセージを抽出し、ソーティングは携帯装置の内部でだけ実行される。勿論、メッセージが極めて長い場合、即ちメッセージが携帯装置のメモリ容量よりをはるかに越える場合、処理回路は、チェックすべきメッセージが通過する際に該メッセージを構成するデータを読み、チェックすべきサインのベースとして役立つデータだけを抽出する。

また、前述のごとく、同一カードが複数のプログラムに対応するサインを含んでいてもよい。これらのサインを識別するために、少なくとも1つのサインを記憶した各プログラムの識別子に関する情報を含むチェック領域を携帯装置に配備してもよい。このチェック領域はまた、所与のオ

リジナルメッセージに関するサインが配置されたメモリアドレスを処理回路に表示してもよい．これは，通し番号でもよくまたは比較されるメッセージの識別を可能にするその他のいかなるタイプの情報でもよい．かかる場合，チェックを行なう際に，システムはチェックすべきメッセージの番号または識別子をユーザーに伝える．

最後に，改良された実施例では，更新のためにメッセージを意図的に変更するときに，携帯装置に記憶された対応する各サインの各々が更新されるように構成されている．この場合，ユーザーの制御下に，変更メッセージに対応する新しいサインの完全な書き替えが携帯装置の別の記憶領域または同じ記憶領域で行なわれる．これは例えばＥＰＲＯＭタイア，即ち携帯装置の回路の制御下に電気的に書き替え及び再プログラミング可能である．メモリカード型携帯装置及び電子マイクロ回路は一般にこの型のメモリを組み込んでおり，これらの携帯装置と外部システムとの間のコネクタの処には，給電及びデータ転送に必要なコネクタに加えて，いくつかのメモリ領域のプログラミングまたは消去用コネクタを配備し得るので，当業者には容易な構造である．その他の例では，プログラミング電圧を携帯装置自体から供給する．しかしながら，どの場合にも，メモリ内での新しいサインの消去及び書き替えは，選択的に行なわれ，変更すべき領域にのみ関係する．

従って本発明は，データ処理記憶媒体に記憶されたプログラム及び/またはデータから成るメッセージの完全性を容易に，安全に且つ比較的廉価に確保し得るので特に有利である．メッセージは，オリジナルからロードされ，ロードされた場所で割込みによって変更されてもよくまたは伝送線路を介して遠隔から変更されてもよい．

勿論，本発明の範囲内で本発明方法及びその実施システムを変更することが可能である．

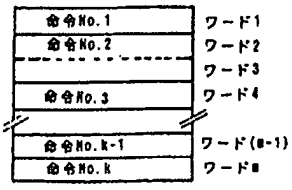

FIG.1A

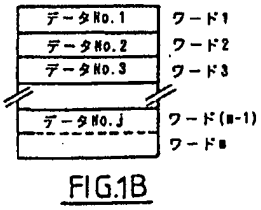

FIG.1B

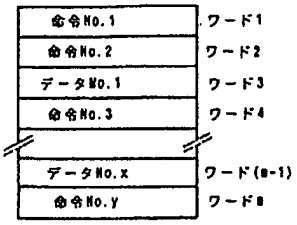

FIG.1C

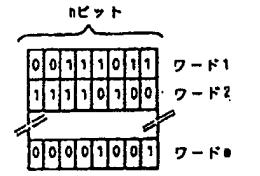

FIG.1D

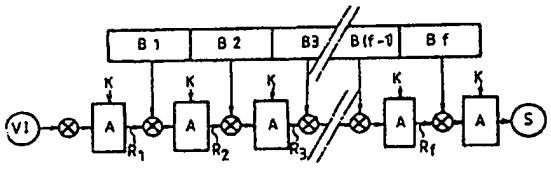

FIG.2

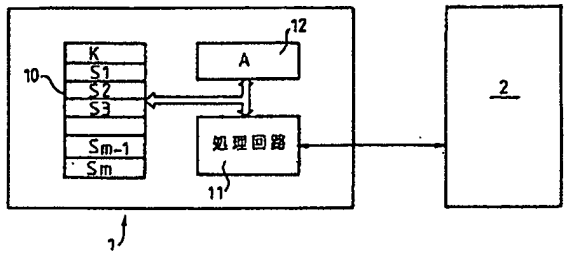

FIG.3

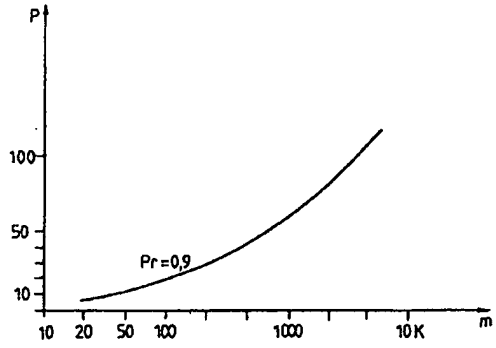

FIG.4

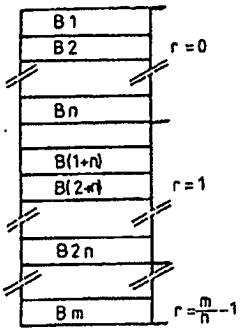

FIG.5

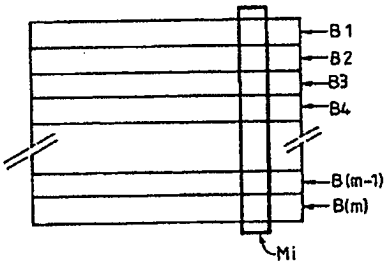

FIG.6

国際調査報告

International Application No PCT/FR 90/00381

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) *

According to International Patent Classification (IPC) or to both National Classification and IPC

Int. Cl.[5] G 06 F 11/06

II. FIELDS SEARCHED

Minimum Documentation Searched *

Classification System	Classification Symbols
Int. Cl.[5]	G 06 F

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched *

III. DOCUMENTS CONSIDERED TO BE RELEVANT *

Category *	Citation of Document, * with indication, where appropriate, of the relevant passages *	Relevant to Claim No. *
Y	EP, A, 0280035 (NIXDORF COMPUTER AG) 31 August 1988, see claim 1	1-4
A	--	6,15,16
Y	IEEE Symposium on Security and Privacy, 18-21 April 1988, Oakland, California, IEEE, M.K. Joseph et al.: "A fault tolerance approach to computer viruses", pages 52-58, see page 54, column 1, lines 2-9; column 2, lines 18-42	1-4
A	--	17,18
A	Proceedings of the 1989 IEEE Computer Society Symposium on Security and Privacy, 1-3 May 1989, Oakland, California, IEEE, G.J. Davida et al.: "Defending systems against viruses through cryptographic authentication", pages 312-318, see page 315, column 1, lines 15-45 ; page 317, column 1, lines 19-28	1-4,8,15,16
A	-- DE, A, 3709524 (ROBERT BOSCH GmbH) 6 October 1988 see abstract	1

* Special categories of cited documents: *
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
4 September 1990 (04.09.90)	3 October 1990 (03.10.90)
International Searching Authority	Signature of Authorized Officer
European Patent Office	

Form PCT/ISA/210 (second sheet) (January 1985)

国際調査報告

FR 9000381
SA 37635

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on 26/09/90
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A- 0280035	31-08-88	DE-A,C 3705736 JP-A- 63240629	01-09-88 06-10-88
DE-A- 3709524	06-10-88	JP-A- 63254548	21-10-88

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82